Manual de configuración del router ZTE ZXHN F8648P de DIGI 10G

redeszone.net/tutoriales/configuracion-routers/zte-zxhn-f8648p-digi-10g-manual/

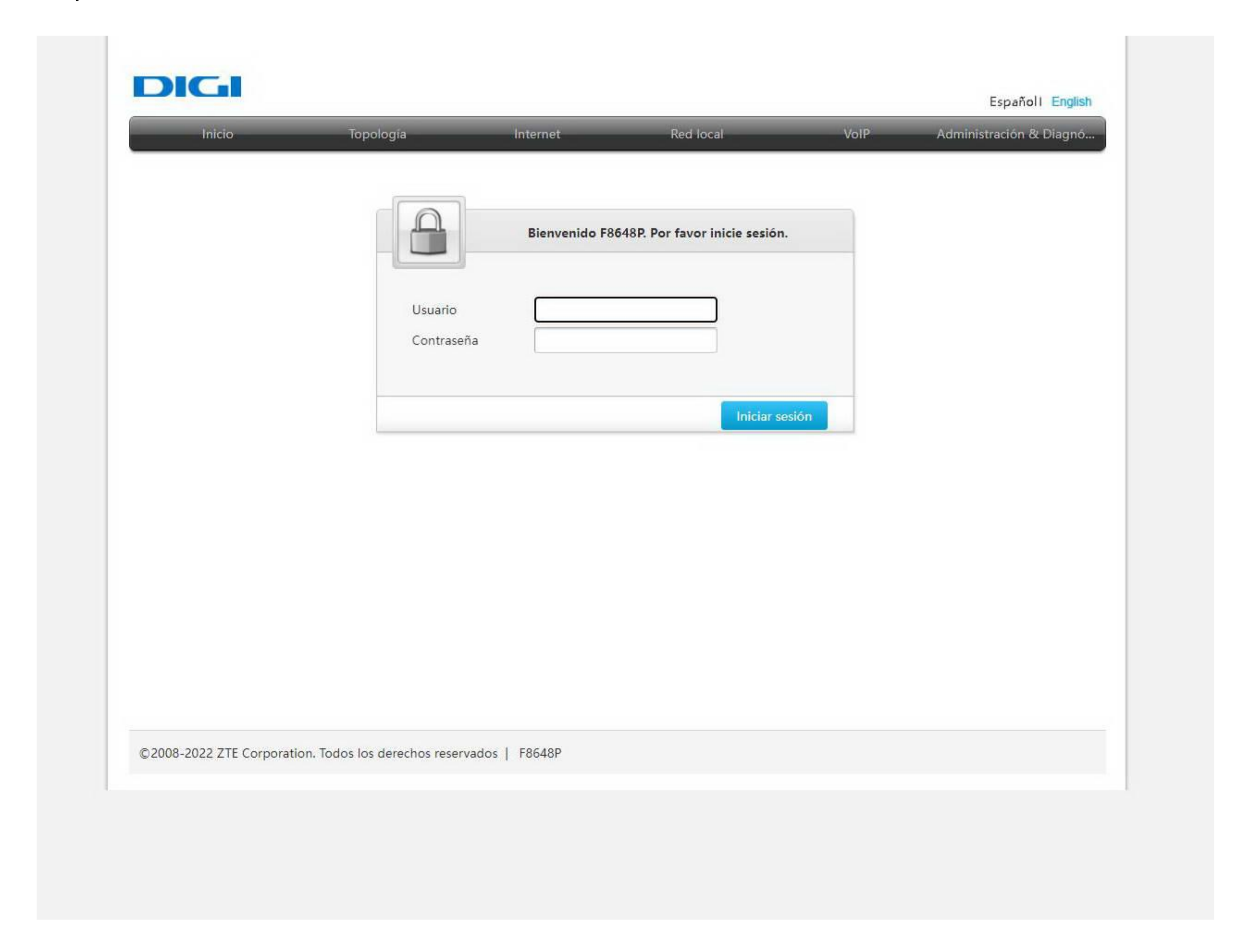


El operador DIGI cuando contratamos la **fibra 10Gb PRO-DIGI** nos instala el router XGS-PON **ZTE ZXHN F8648P**, aunque en el pasado también ha instalado otro modelo de la marca ZyXEL con especificaciones similares. Este router incorpora la ONT integrada, y nos permitirá conseguir una velocidad real de hasta 8Gbps simétricos por cable, ya que tiene un puerto 10GBASE-T Multigigabit de alto rendimiento, perfecto para no tener cuello de botella en la red LAN. Si tienes esta conexión del operador DIGI y te han instalado este router, hoy os vamos a enseñar las **principales configuraciones que deberías realizar (en modo usuario)**, y también os enseñaremos cómo ponerlo en modo bridge o puente, aunque esto último es bastante complicado para cualquier usuario normal, ya que hay que usar Linux para poder realizar el proceso.

El operador DIGI no pone nada fácil la posibilidad de entrar al router en modo administrador y poder configurar cualquier opción, por defecto, tenemos un usuario «user» pero siguiendo una serie de pasos complejos, podemos iniciar sesión como administrador y entonces sí podemos realizar todas las configuraciones de las que dispone el router del fabricante ZTE. Durante todo el tutorial os vamos a enseñar los menús en modo usuario, excepto para ponerlo en modo puente donde usaremos el modo de configuración de administrador.

Acceso al firmware de configuración vía web

El router de DIGI se administra como cualquier otro router del operador, en este caso, debemos acceder vía web con cualquier navegador a la dirección **http://192.168.1.1** como suele ser habitual. Una vez que estemos dentro, tendremos que utilizar el nombre de usuario «**user**» y la contraseña «**user**«, ya que es predeterminada, pero posteriormente podremos cambiar esta contraseña para gestionar el router. Hay que tener en cuenta que estas credenciales nos dan acceso a todos los menús de configuración del router, excepto los ocultados por el operador y que solamente están disponibles en el modo administrador.

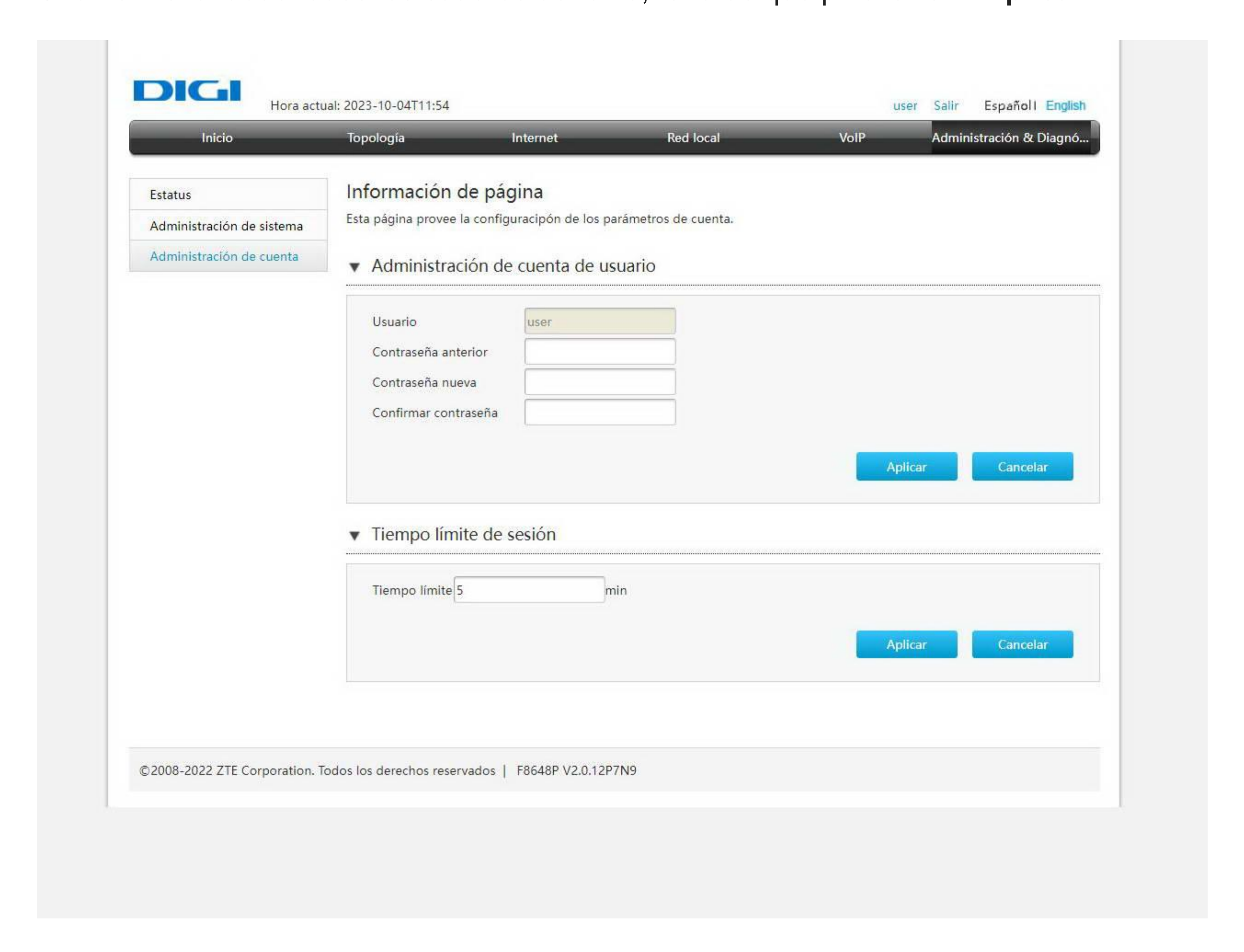


Ahora que ya sabéis cómo acceder al router de DIGI, vamos a ver cómo cambiar la contraseña de acceso al router para estar más protegidos y que nadie pueda meterse en su administración en modo usuario.

Cambio de la contraseña de acceso

Si quieres cambiar la contraseña de acceso, deberás irte a la sección de «**Administración & Diagnóstico**«, en la sección de «**Administración de cuenta**» es donde tendremos que cambiar la contraseña correspondiente al usuario «**user**«, tal y como podéis ver.

Para cambiar la contraseña, tendremos que introducir la contraseña anterior, si es la predeterminada tendrás que poner «**user**» como contraseña anterior. Una vez introducida la clave anterior, tendrás que poner la nueva contraseña que quieras usar tanto en el cuadro de texto «**Contraseña nueva**» como en «**Confirmar contraseña**«. Una vez rellenadas todos los cuadros de texto, tendrás que pinchar en «**Aplicar**«.



También podrías cambiar el tiempo límite de sesión, por defecto está en 5 minutos que es más que suficiente para realizar cualquier tipo de configuración, pero puedes disminuir este tiempo o aumentarlo, y posteriormente pinchar en «Aplicar».

Configuración de la red Wi-Fi

La red Wi-Fi en los routers es una de las partes fundamentales, ya que la mayoría de clientes que conectemos al equipo será de manera inalámbrica, usando portátiles, Smart TV, smartphones, tablets e incluso dispositivos domóticos para el hogar que usan la banda de 2.4GHz. Este router dispone del **estándar Wi-Fi 6**, por lo que tendremos una muy buena cobertura y también una gran velocidad, sobre todo en lugares cercanos al router principal, ya que **hemos conseguido más de 1000Mbps reales de descarga y más de 1.400Mbps de subida**, perfecto para que la navegación y la descarga o subida de archivos sea realmente ágil.

Aunque la mayoría de fabricantes de routers y de operadores han habilitado la **función de band-steering**, para tener un único SSID compartido con las dos bandas de frecuencias (2.4GHz y 5GHz), en **DIGI han decidido separar las bandas de forma predeterminada**, con el objetivo de no tener problemas al conectar dispositivos de domótica, y que los usuarios sepan en todo momento a qué bandas de frecuencias se conectan. Creemos que esta configuración que ha elegido DIGI es perfecta. En el caso de que estés interesado en tener el band-steering, lo podrás activar en la web de administración del router, pero no os lo recomendamos por todos los problemas que podrías tener. Si quieres conocer todas las opciones de configuración disponibles, a continuación, os las vamos a explicar en detalle.

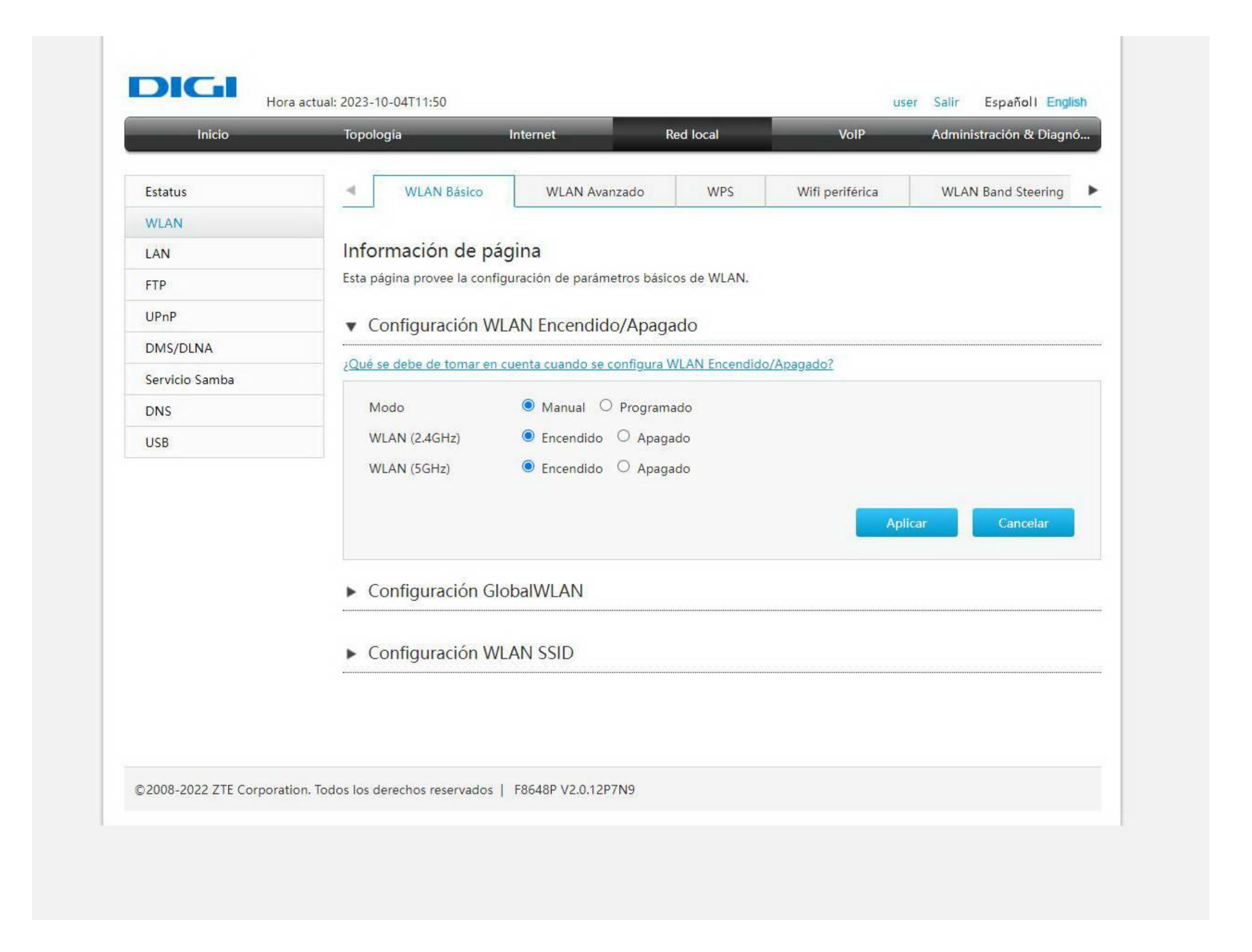
En la sección de «**Red local / WLAN**» es donde tenemos todas las opciones de configuración disponibles relacionadas con la red inalámbrica.

WLAN Básico

En este menú de WLAN Básico podemos realizar todos los ajustes necesarios de la red inalámbrica Wi-Fi, concretamente, podemos realizar:

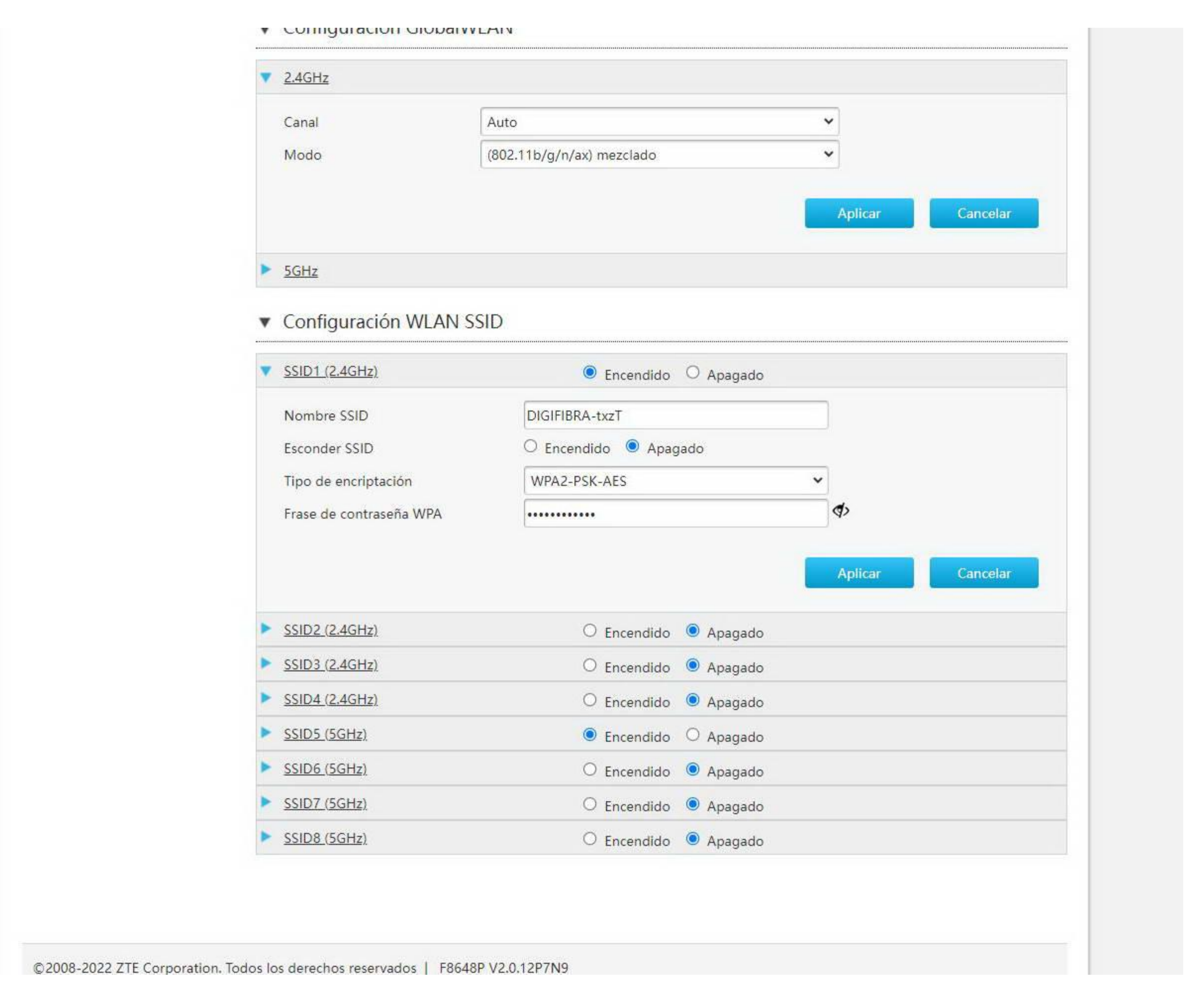
Configuración WLAN Encendido/Apagado: en este menú podemos configurar si queremos encender o apagar la red inalámbrica de forma manual, o bien en función de una programación determinada. Si eres de los que apagan el WiFi por las noches, entonces tendrás que pinchar en el botón de «Modo: Programado» para realizar los ajustes necesarios.

- **Modo**: permite configurar «Manual» y «Programado», dependiendo de lo que quieras hacer, tendrás que elegir una opción u otra.
- **WLAN 2.4GHz**: permite configurar «Encendido» y «Apagado». Lo normal es tener esta banda de frecuencias siempre habilitada, en caso de que quieras apagarla, tendrás que pinchar en «Apagado».
- **WLAN 5GHz**: permite configurar «Encendido» y «Apagado». Lo normal es tenerla siempre habilitada, en caso de que quieras apagarla, tendrás que pinchar en «Apagado».



Configuración WLAN GlobalWLAN: en este menú podemos configurar a nivel de radio las dos bandas de frecuencias, lo cierto es que tenemos pocas opciones de configuración, solamente podemos editar el canal de emisión y el modo de emisión de Wi-Fi para proporcionar compatibilidad hacia atrás.

- **2.4GHz**:
  - **Canal**: por defecto el canal elegido está en automático, pero podemos elegir el que nosotros queramos.
  - **Modo**: por defecto está en 802.11b/g/b/ax para proporcionar compatibilidad con todos los clientes, tanto los nuevos como los antiguos.
- **5GHz**:
  - **Canal**: por defecto el canal elegido está en automático, pero podemos elegir los canales «bajos» del 36-48 y también los canales DFS de cualquier frecuencia.
  - **Modo**: 802.11b/g/b/ax por defecto para proporcionar compatibilidad con todos los clientes.



Configuración WLAN SSID: en este menú podemos configurar el nombre de la red WiFi y su seguridad. Tenemos a nuestra disposición la gran mayoría de opciones de configuración de siempre. Las opciones disponibles para la banda de 2.4GHz y de 5GHz son exactamente las mismas, no hay diferencia.

- **Nombre SSID**: es el nombre de la red WiFi, la que veremos a la hora de conectarnos con los dispositivos inalámbricos.
- **Esconder SSID**: lo normal es tenerlo «Apagado», no proporciona ningún tipo de seguridad ocultar el SSID, de hecho, es incluso peor para la privacidad.
- **Tipo de encriptación**: es el protocolo elegido para la autenticación, por defecto es WPA2-PSK AES, y es una opción correcta hoy en día para tener la máxima compatibilidad posible.
- **Frase de contraseña WPA**: es la contraseña de acceso a la red WiFi, debe tener entre 8 y 63 caracteres.

▼ Configuración WLAN SSID

SSID1 (2.4GHz)	◉ Encendido ○ Apagado	
Nombre SSID	DIGIFIBRA-txzT	
Esconder SSID	○ Encendido ◉ Apagado	
Tipo de encriptación	WPA2-PSK-AES	
Frase de contraseña WPA	••••••••••••	
	Aplicar	Cancelar
SSID2 (2.4GHz)	○ Encendido ◉ Apagado	
SSID3 (2.4GHz)	○ Encendido ◉ Apagado	
SSID4 (2.4GHz)	○ Encendido ◉ Apagado	
SSID5 (5GHz)	◉ Encendido ○ Apagado	
Nombre SSID	DIGIFIBRA-PLUS-txzT	
Esconder SSID	○ Encendido ◉ Apagado	
Tipo de encriptación	WPA2-PSK-AES	
Frase de contraseña WPA	••••••••••••	
	Aplicar	Cancelar
SSID6 (5GHz)	○ Encendido ◉ Apagado	
SSID7 (5GHz)	○ Encendido ◉ Apagado	
SSID8 (5GHz)	○ Encendido ◉ Apagado	

En la siguiente imagen podéis ver las opciones para la banda de 5GHz:

▼ Configuración WLAN SSID

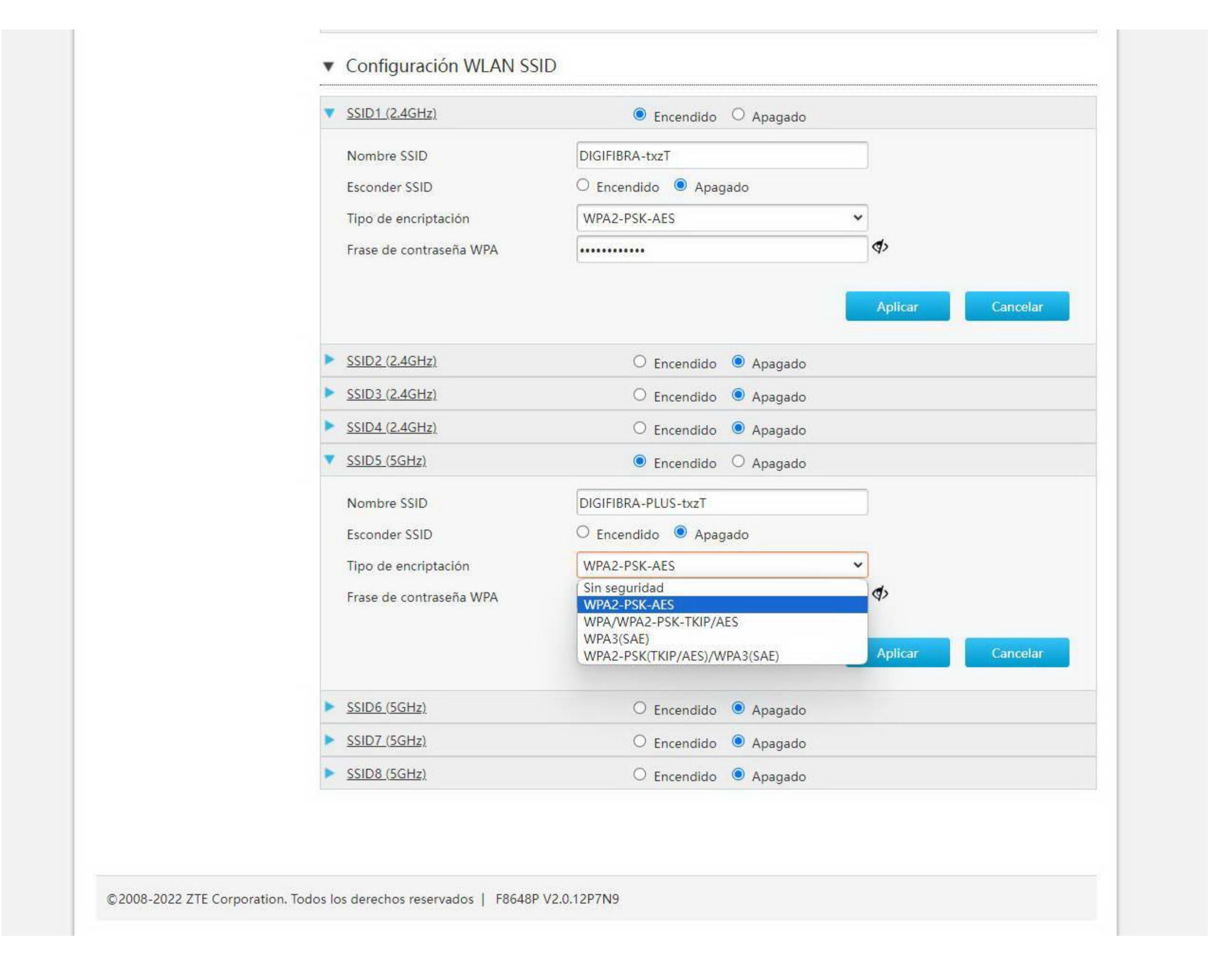
SSID1 (2.4GHz)	◉ Encendido ○ Apagado	
Nombre SSID	DIGIFIBRA-txzT	
Esconder SSID	○ Encendido ◉ Apagado	
Tipo de encriptación	WPA2-PSK-AES	
Frase de contraseña WPA	••••••••••••	
	Aplicar	Cancelar
SSID2 (2.4GHz)	○ Encendido ◉ Apagado	
SSID3 (2.4GHz)	○ Encendido ◉ Apagado	
SSID4 (2.4GHz)	○ Encendido ◉ Apagado	
SSID5 (5GHz)	◉ Encendido ○ Apagado	
Nombre SSID	DIGIFIBRA-PLUS-txzT	
Esconder SSID	○ Encendido ◉ Apagado	
Tipo de encriptación	WPA2-PSK-AES	
Frase de contraseña WPA	••••••••••••	
	Aplicar	Cancelar
SSID6 (5GHz)	○ Encendido ◉ Apagado	
SSID7 (5GHz)	○ Encendido ◉ Apagado	
SSID8 (5GHz)	○ Encendido ◉ Apagado	

©2008-2022 ZTE Corporation. Todos los derechos reservados | F8648P V2.0.12P7N9

Este router soporta otros tipos de cifrados para la red inalámbrica Wi-Fi, a continuación, os explicamos cuáles son y cuál debemos elegir:

- **Sin seguridad**: no tendremos contraseña de acceso, cualquiera dentro del rango de cobertura podría conectarse a la red inalámbrica. No es recomendable usar esta opción.
- **WPA2-PSK AES**: es un tipo de cifrado muy seguro hoy en día, aunque hay algunos ataques que podrían vulnerar la contraseña, si eliges una contraseña larga de más de 15 caracteres no deberías tener ningún problema.
- **WPA/WPA2-PSK TKIP/AES**: no es recomendable usar este tipo de cifrado porque permite conectarnos con WPA-TKIP que es un protocolo no seguro.
- **WPA3 (SAE)**: es el último protocolo de seguridad WiFi, es el más seguro de todos porque además tendremos las tramas de administración protegidas para evitar ataques de denegación de servicio a los clientes WiFi, impide que se pueda conseguir la contraseña offline mediante fuerza bruta y diccionario etc. Lo peor es que no todos los clientes inalámbricos soportan este estándar, y los que no lo soporten no podrán conectarse, por lo tanto, debes asegurarte que todos tus clientes sí lo soportan para usarlo.
- **WPA2-PSK(TKIP/AES)/WPA3(SAE)**: teniendo en cuenta que se podría usar WPA-TKIP, no os recomendamos usarlo. Además, no tendremos una mayor seguridad por el hecho de poder seleccionar WPA3, ya que hay ataques de «downgrade» que permiten forzar el protocolo más débil. No uses esta opción.

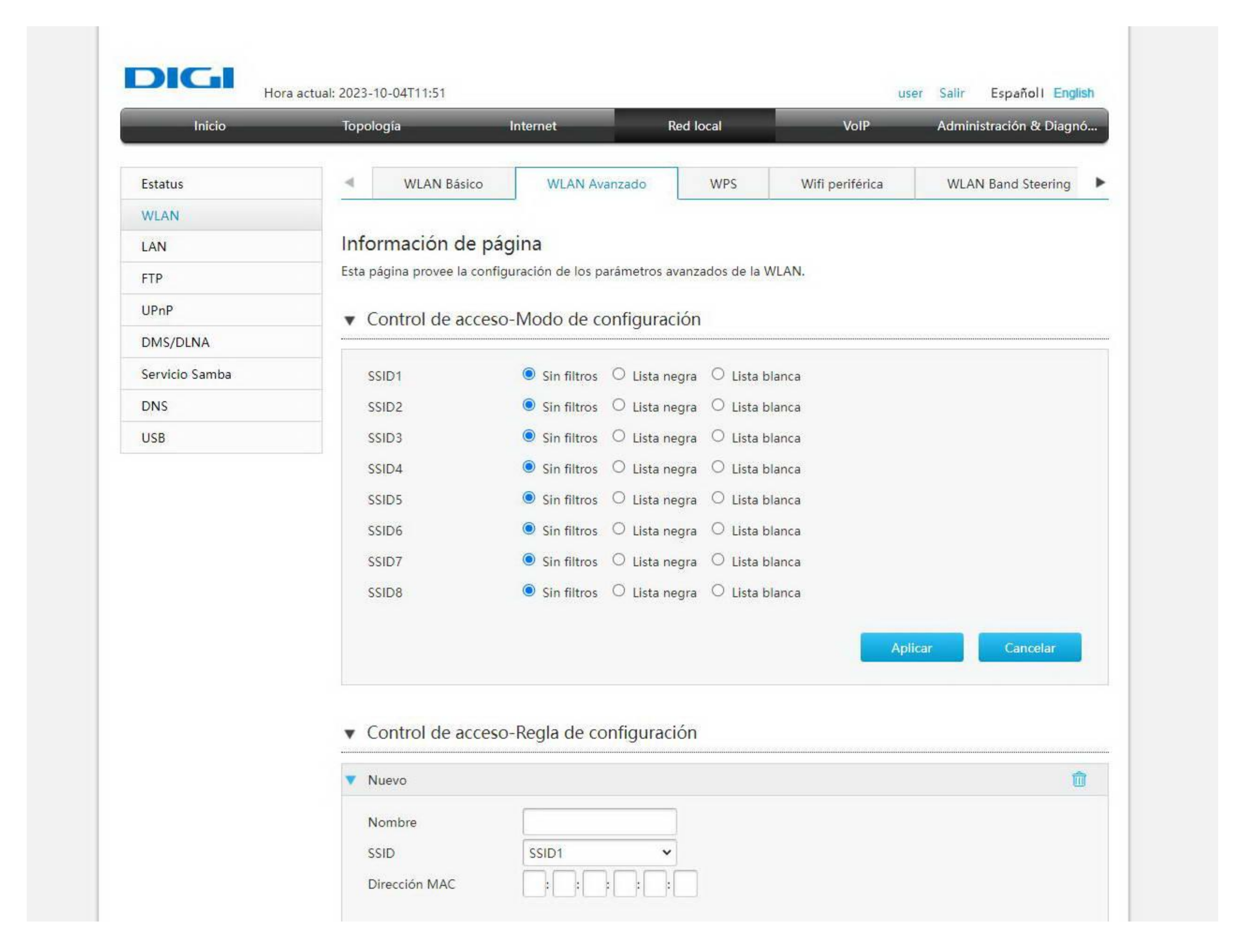
En definitiva, para tener la mejor seguridad deberías usar WPA2-PSK AES que viene por defecto, o bien usar WPA3 (SAE) si todos tus clientes inalámbricos lo soportan. Si no lo soportan todos los clientes WiFi, entonces no lo uses porque no podrán conectarse.



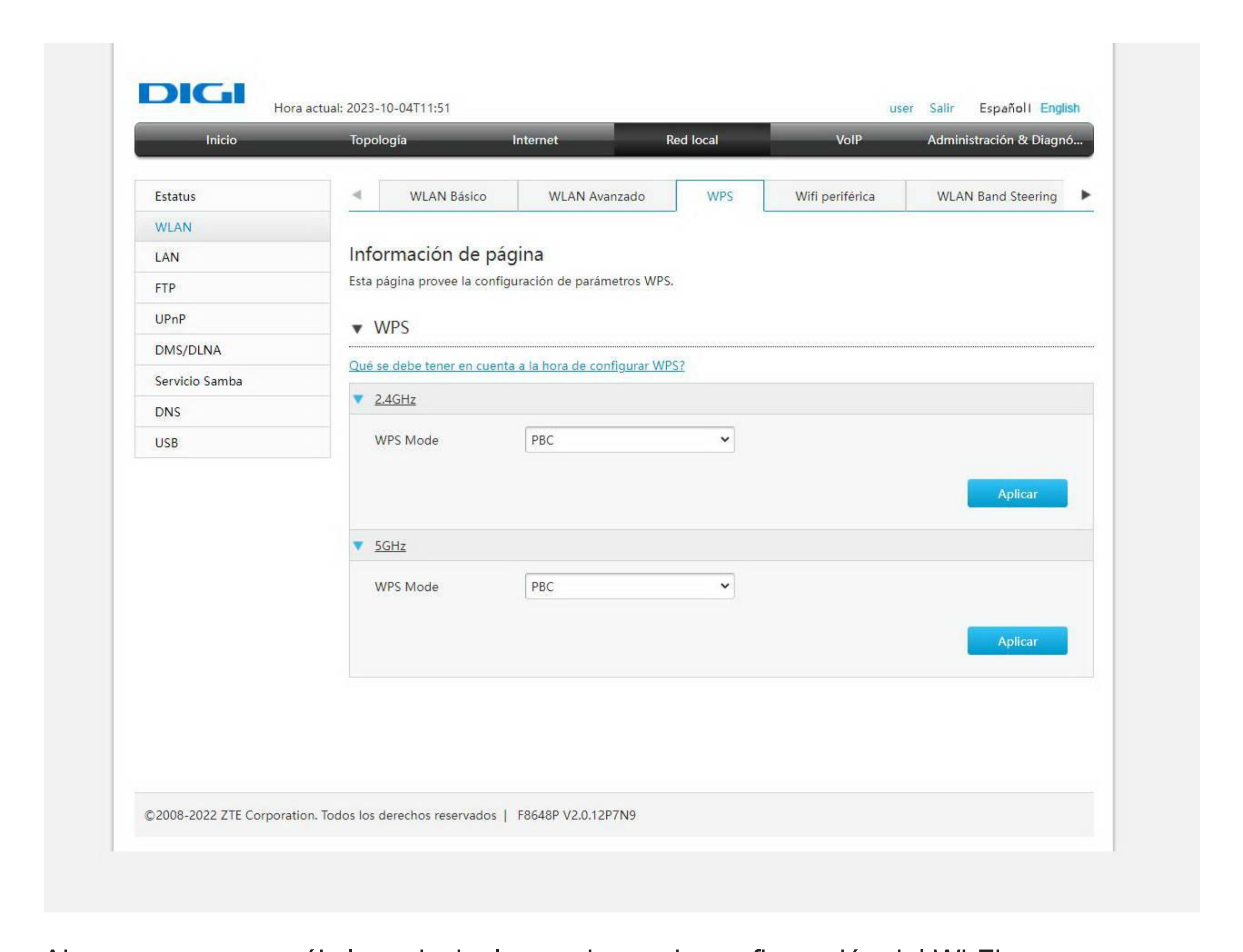
Tal y como podéis ver, tenemos a nuestra disposición muchas opciones de configuración para personalizar la red inalámbrica en detalle.

WLAN Avanzado y más

En el menú de WLAN Avanzado es donde puedes configurar el filtrado MAC, tenemos la posibilidad de configurar tanto una lista negra como una lista blanca, y todo ello para los ocho SSID que podemos crear. Nuestra recomendación es que no uses el filtrado MAC porque no aporta realmente ninguna seguridad adicional, ya que la dirección MAC WiFi se puede clonar muy fácilmente.



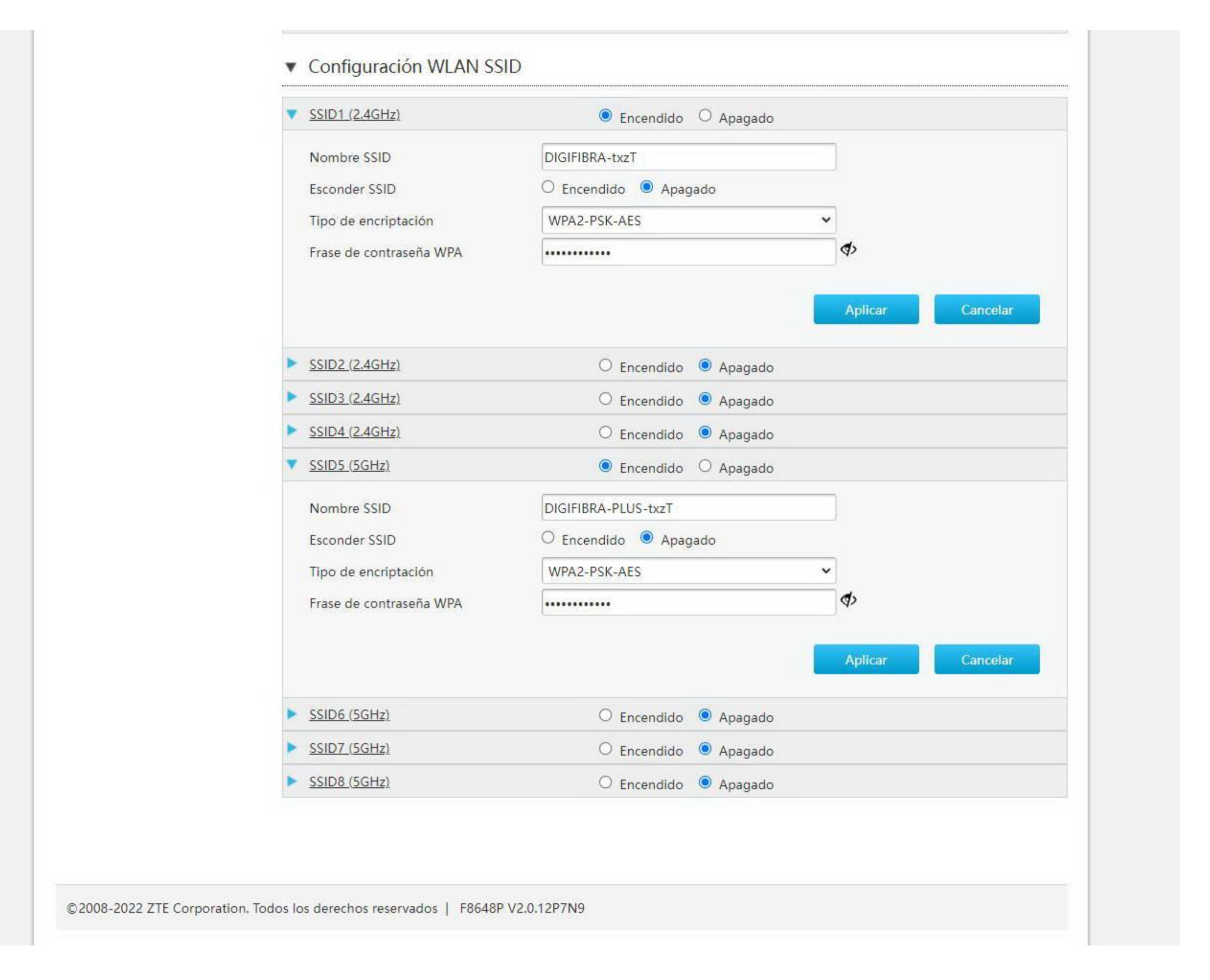
En el caso del WPS, el funcionamiento es solamente a través del botón físico. Este modo de configuración es bastante seguro porque tendremos que pulsar nosotros el botón, y no tendremos el típico PIN de 8 dígitos. No obstante, nuestra recomendación es que nunca utilices dicho botón WPS para dar de alta los diferentes dispositivos inalámbricos, es mejor poner la contraseña directamente para no tener que tener un cierto espacio de tiempo donde alguien puede conectarse u obtener la contraseña WPA2. Si eliges el protocolo WPA3(SAE) el botón WPS no funcionará, ya que no forma parte del estándar, esto también debes tenerlo en cuenta.



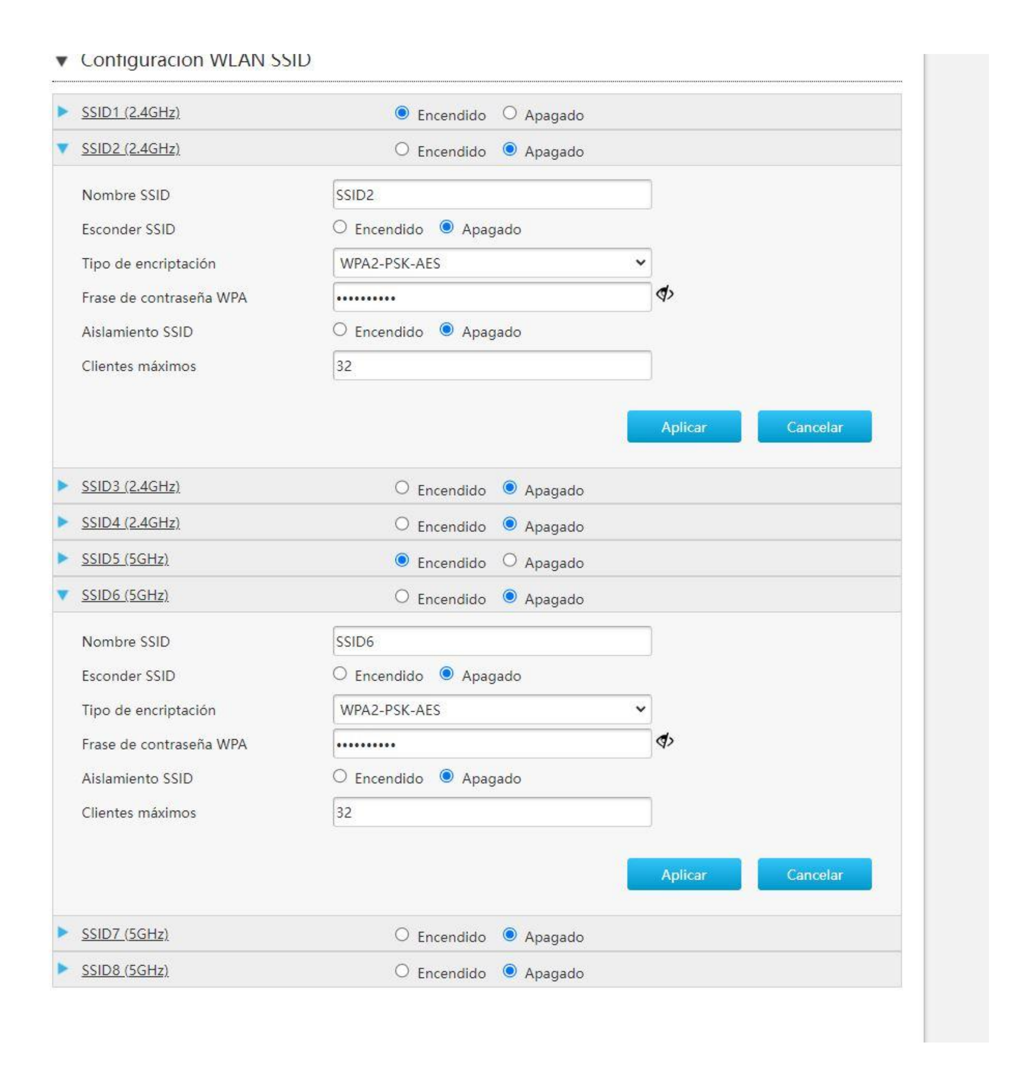
Ahora que ya conocéis las principales opciones de configuración del Wi-Fi, os vamos a enseñar cómo crear una segunda red para usarla como red Wi-Fi de invitados. Aunque también tenemos la pestaña de «**WLAN Band steering**» no es necesario que configuremos nada, porque por defecto esta funcionalidad se encuentra desactivada para separar las bandas de frecuencias en SSID diferentes, perfecto para no tener problemas con los dispositivos de la domótica en el hogar.

Configurar la red WiFi de invitados

Echamos de menos que ZTE no tenga un menú específico para la red WiFi de invitados, y que sea muy fácil su activación. Para poder configurar una red WiFi de invitados tienes que meterte en la sección de «Configuración WLAN SSID» que hemos visto antes, justo al lado de los SSID predeterminados de la red principal:



Si desplegamos el SSID2 podremos ver que tenemos la posibilidad de crear un nuevo SSID con otro nombre de red, tipo de cifrado y la contraseña correspondiente. Este SSID2 está específicamente diseñado para la banda de 2.4GHz, por lo que solamente emitirá aquí. Si desplegamos el SSID 6 tendremos la nueva red WiFi que está dedicada específicamente a la banda de 5GHz, por lo que este SSID solamente emitirá también en esta banda únicamente.



Cuando creamos un SSID de invitados, tenemos la posibilidad de habilitar el «**Aislamiento SSID**«, esto significa que los clientes inalámbricos no se podrán comunicar entre ellos, con el objetivo de proporcionar una mejor privacidad y seguridad a dichos clientes. Aunque no tenemos ninguna opción para prohibir acceso a la red principal, lo cierto es que no tenemos acceso a los equipos conectados en la red inalámbrica principal, perfecto para tener la seguridad necesaria.

Ahora que ya habéis visto todas las opciones de configuración del Wi-Fi, vamos a ver otras opciones habituales que puedes hacer en el router.

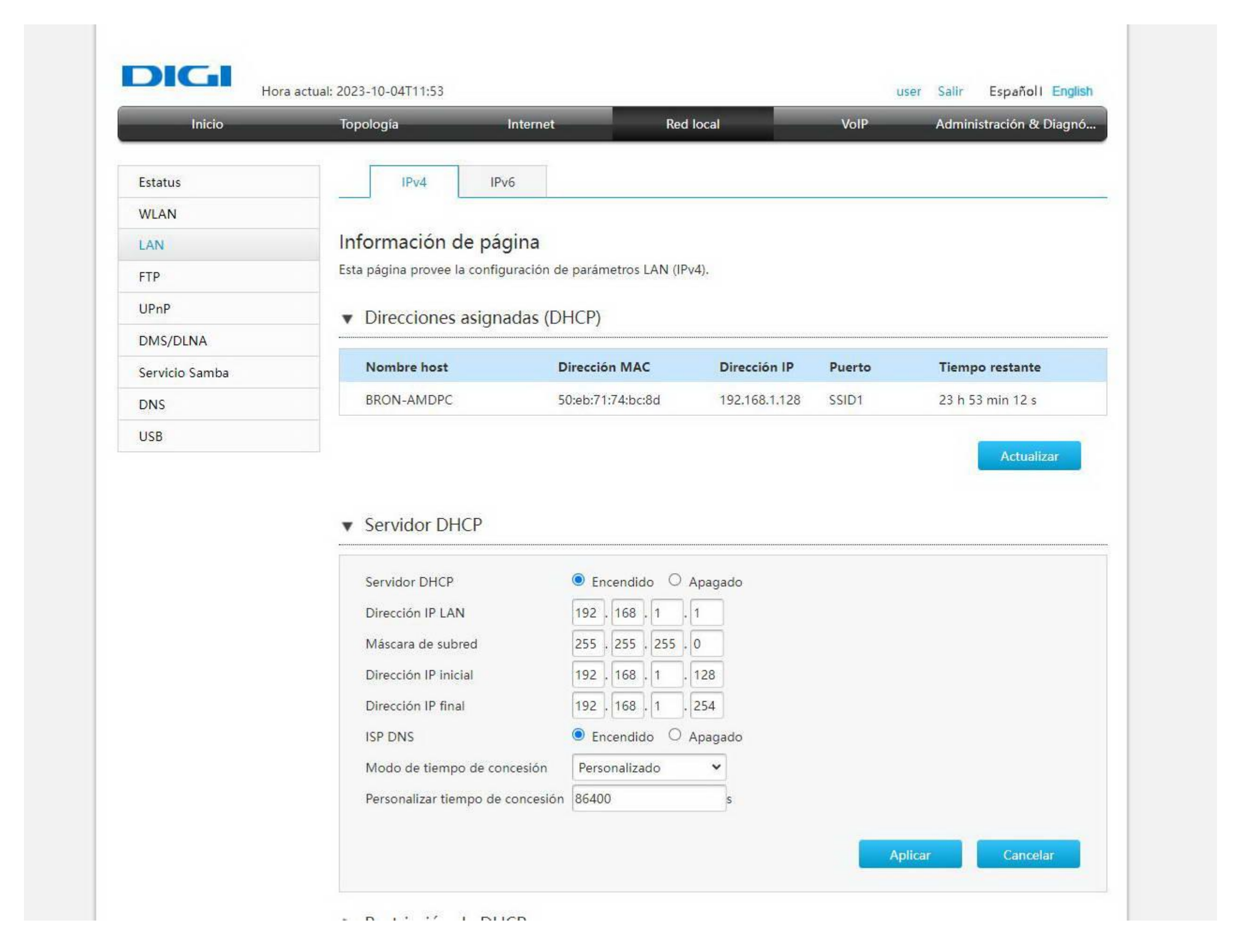
Poner IP privada fija a cualquier dispositivo

Si quieres que todos tus dispositivos siempre tengan la misma dirección IP privada, con el objetivo de poder abrir puertos en la NAT y no tener problemas porque cambie la dirección IP pública, tienes que irte a la sección de «**Red local**«, y en el menú de «**LAN**» es donde debes realizar las configuraciones. En este menú tendremos tanto el **protocolo IPv4 como IPv6**, hay que recordar que DIGI proporciona por defecto una **IPv4 dentro de CG-NAT** (que podemos salir por 1€ mensual con su conexión Plus), y también un direccionamiento IPv6 para conectarnos con una IP Global Unicast Address por cada cliente que conectemos.

¿Para qué tengo que poner una dirección IP privada fija en mis dispositivos de la red local? Los motivos son los siguientes:

- Si quieres abrir puertos TCP y UDP, hay tener IP fija para que el DHCP no cambie la IP privada. Si cambia la IP la apertura de puertos hacia esa IP en concreto no servirá de nada.
- Si quieres compartir archivos en la red local, con un PC o NAS, tendrás que poner IP fija para que no cambie nunca y puedas configurar los anclajes de red en los diferentes sistemas.
- Si vas a jugar con consolas o PC, tendrás que tener IP fija para abrir los puertos bien y no tener problemas.

Seleccionamos la pestaña de «**IPv4**» y podremos ver las direcciones asignadas por el servidor DHCP actual, y también podemos ver la configuración del servidor DHCP en concreto. Por defecto tenemos la típica configuración con un rango desde .128 hasta la IP .254.

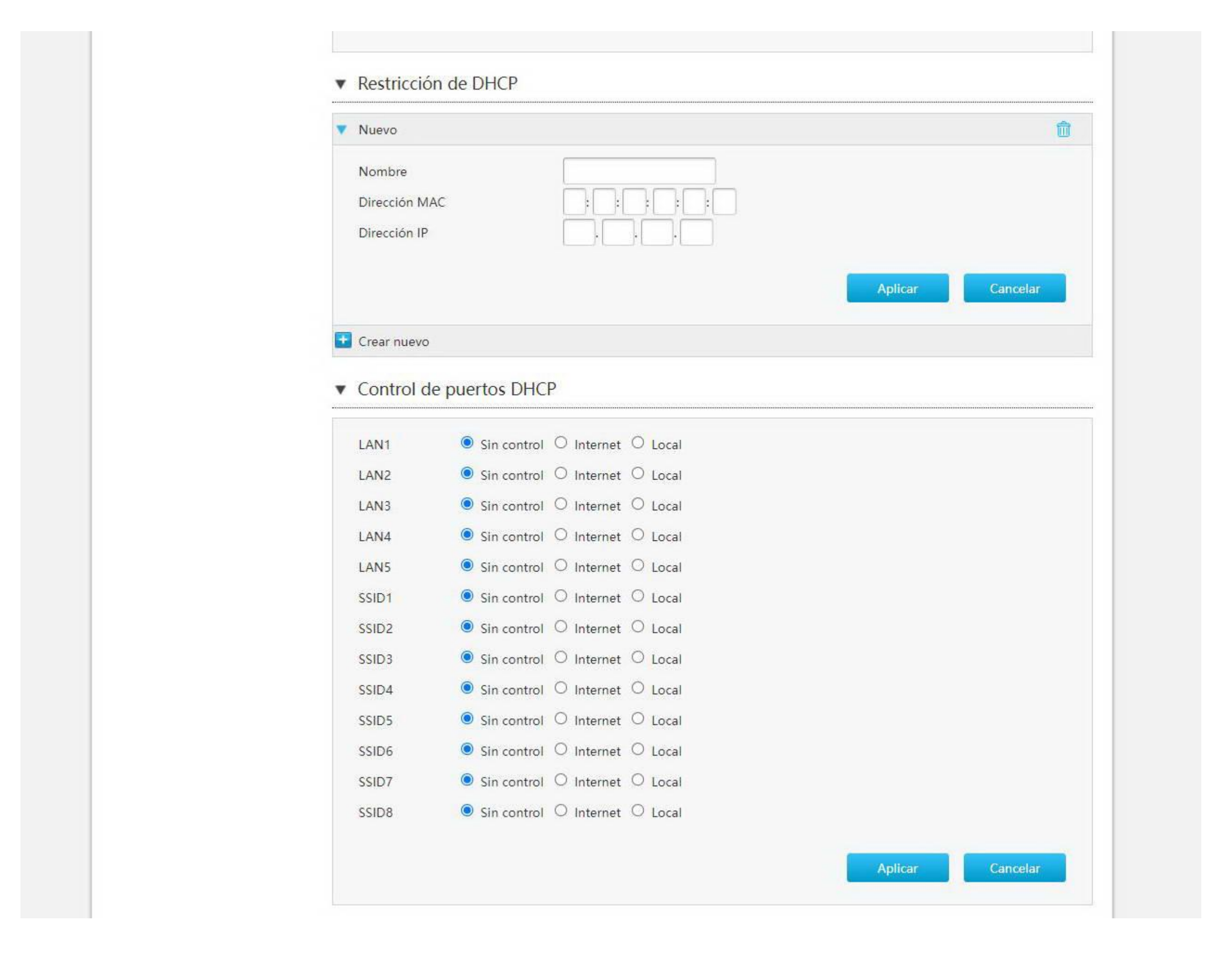


Justo debajo de estas configuraciones tendremos la sección de «**Restricción de DHCP**«, donde debes realizar las configuraciones pertinentes. En esta sección tendrás que poner:

- **Nombre**: el nombre del host.

- **Dirección MAC**: debemos poner la dirección MAC de la tarjeta de red, ya sea cableada o WiFi. Para poder ver la dirección MAC, tenemos la posibilidad de verla en el listado de clientes DHCP conectados que tenemos en la parte superior. Si nunca se ha conectado al router, entonces puedes optar por abrir un símbolo del sistema en Windows (CMD), y poner la orden «ipconfig /all» y elegir la tarjeta de red que vayas a conectar.
- **Dirección IP**: debemos poner la dirección IP privada fija que nosotros queramos, y que no cambiará.

Una vez que lo hayamos rellenado todo, pinchamos en «Aplicar» y tendremos la primera regla. El router nos permite añadir varios dispositivos simultáneamente, no hay problema por poner varios.



Este paso es fundamental para poder abrir puertos en el router correctamente.

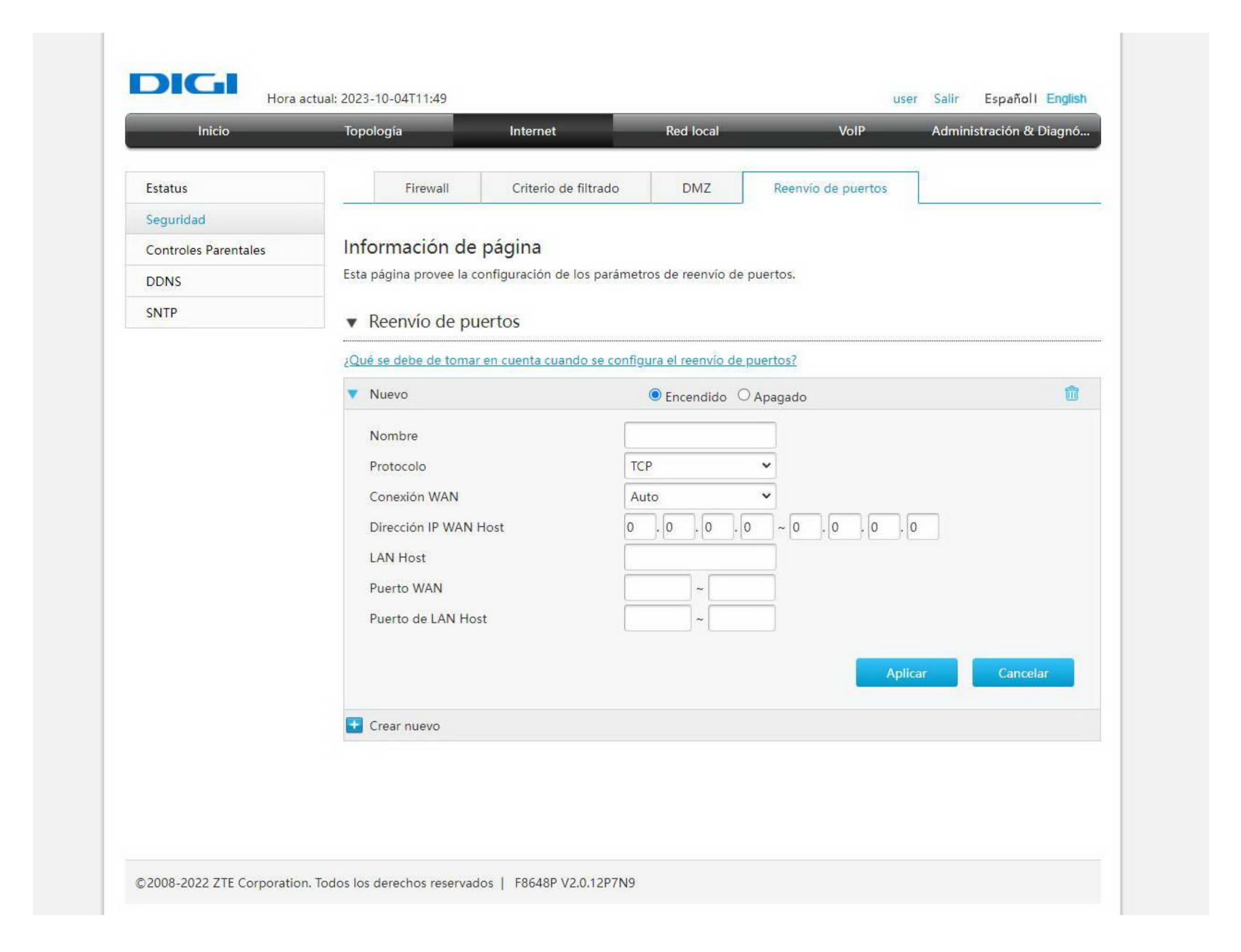
Abrir puertos en el router

Una de las partes más importantes en la configuración de cualquier router es abrir puertos en la NAT, o mejor dicho, configurar el «Reenvío de puertos» o también conocido como «Port Forwarding». El operador DIGI pone a todos sus clientes de forma predeterminada bajo el CG-NAT, es decir, nos proporcionará una dirección IP privada en la WAN de Internet, y esta IP no es enrutable en Internet, por lo que, aunque abramos los

puertos no podrán comunicarse con nosotros. Es necesario llamar a DIGI y contratar la conexión Plus por 1€ más al mes, y de esta forma, tener una dirección IPv4 pública para nosotros solos.

Una vez que tengas IPv4 pública en la WAN de Internet, para abrir puertos debes irte a la sección de «**Internet / Seguridad / Reenvío de puertos**«. En este menú podemos añadir diferentes reglas para abrir los puertos que nosotros queramos. Las opciones que debemos rellenar son las siguientes:

- **Nombre**: simplemente ponemos un nombre descriptivo de qué estamos abriendo. Si vas a abrir el servidor FTP o VPN, puedes ponerlo tal cual.
- **Protocolo**: podemos elegir entre protocolo TCP, UDP o ambos (TCP y UDP).
- **Conexión WAN**: podemos dejarlo en «Auto» o bien elegir nuestra conexión INTERNET.
- **Dirección IP WAN Host**: lo dejamos con todo 0, esto significa que acepta desde cualquier dirección IP de origen, debemos dejarlo por defecto.
- **LAN Host**: debemos poner la dirección IP privada de nuestro PC, consola o NAS. Si has puesto IP privada fija como os hemos enseñado antes, no tendrás problemas.
- **Puerto WAN**: aquí debemos introducir el puerto a abrir en la WAN de Internet. Si queremos abrir un único puerto, ponemos el mismo número en ambas casillas. Si queremos abrir un rango desde el 40000 hasta el 40010 (por ejemplo), ponemos tanto el inicio como el final.
- **Puerto LAN**: aquí debemos introducir el puerto a abrir en la LAN, generalmente es el mismo que en la WAN de Internet. Si queremos abrir un único puerto, ponemos el mismo número en ambas casillas. Si queremos abrir un rango, lo hacemos como antes.



Imaginemos que queremos abrir el puerto del servidor OpenVPN que usa UDP en el puerto 1194 por defecto, hacia nuestro NAS con la IP 192.168.1.10. La configuración que debemos realizar es la siguiente:

- **Nombre**: servidor OpenVPN
- **Protocolo**: UDP
- **Conexión WAN**: podemos dejarlo en «Auto» o bien elegir nuestra conexión INTERNET.
- **Dirección IP WAN Host**: 0.0.0.0 – 0.0.0.0
- **LAN Host**: 192.168.1.10
- **Puerto WAN**: 1194 – 1194
- **Puerto LAN**: 1194 – 1194

Una vez hecho, pinchamos en «Aplicar» y ya habremos dado de alta la nueva regla. Como podéis ver, en este router es realmente sencillo abrir puertos.

Abrir la DMZ en el router para la consola o PC

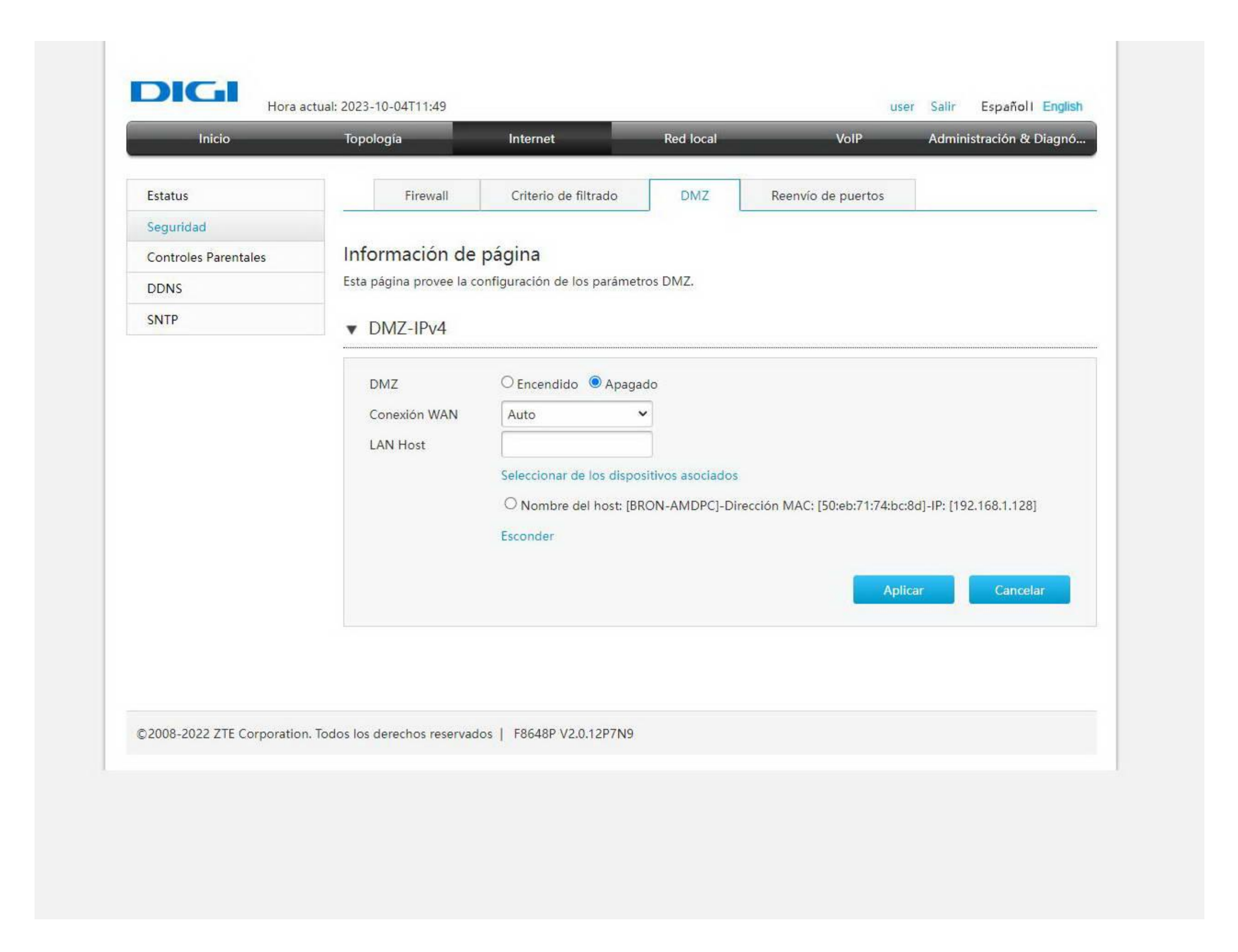
La funcionalidad de DMZ nos permite abrir todos los puertos excepto los que tengamos abiertos de manera específica. Esto es perfecto para abrir todos los puertos hacia nuestra consola de juegos o el PC, no obstante, hay que usarlo con cuidado porque

estamos abriendo todos los puertos a Internet. En el caso de que sea una consola no hay mucho problema ya que están preparadas para ello, pero si lo haces en un PC deberías tener un firewall para impedir las conexiones remotas.

En este caso, para que la DMZ funcione también es completamente necesario que tengamos una dirección IPv4 pública en la WAN de Internet, y no estar dentro de CG-NAT porque no servirá de nada abrir la DMZ en este caso. Una vez que tengas IPv4 pública en la WAN de Internet, para abrir la DMZ debes irte a la sección de «**Internet / Seguridad / DMZ**«.

En este menú, tendrás que realizar las siguientes configuraciones:

- **DMZ**: encendido o apagado. Si la queremos habilitar debemos pinchar en «Encendido».
- **Conexión WAN**: podemos dejarlo en «Auto» o bien elegir nuestra conexión INTERNET.
- **LAN Host**: tenemos que poner la dirección IP privada a la que queramos abrir la DMZ.

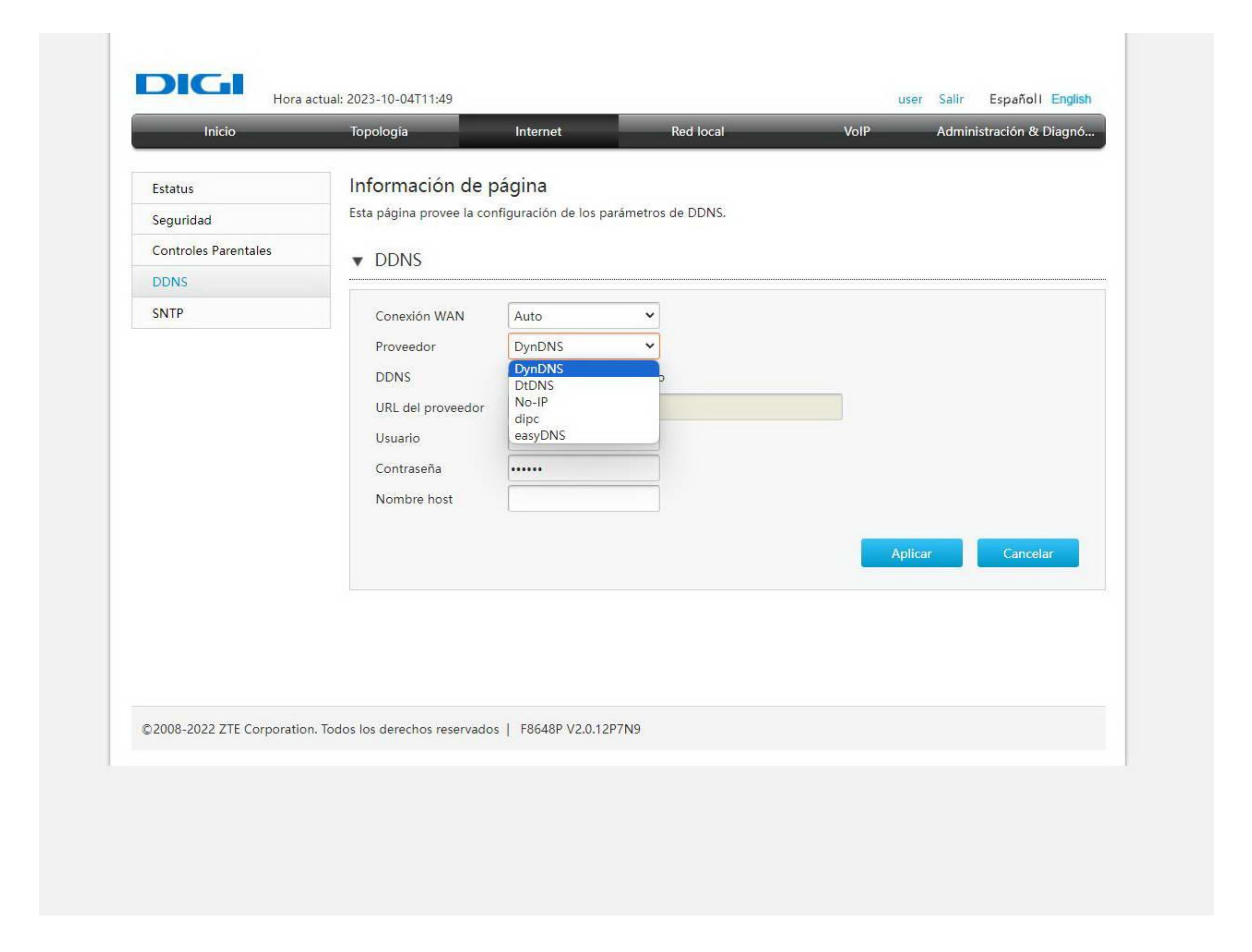


Justo debajo nos saldrán el listado de todos los clientes cableados e inalámbricos que tengamos conectados, para facilitarnos la elección de los diferentes clientes. Pero también podemos ponerlo de manera manual indicando la dirección IPv4.

Configurar el DNS dinámico o DynDNS

La conexión PPPoE de DIGI nos proporciona una dirección IP dinámica, esto significa que con cada conexión la IP pública cambiará, no es fija. Para poder acceder a los recursos de la red local, lo más recomendable es usar el host de DNS dinámico, para que siempre tengamos localizada nuestra conexión a Internet. Si quieres usar un host de DNS dinámico, deberás irte a la sección de «**Internet / DDNS**«, en este menú debemos elegir las siguientes opciones:

- **Conexión WAN**: auto o elegimos INTERNET.
- **Proveedor**: elegimos el proveedor del servicio que tengamos.
- **URL del proveedor**: algunos DDNS necesitan que pongamos una URL para actualizar la dirección IP pública, no todos, pero algunos sí.
- **Usuario**: el nombre de usuario de acceso al host de DDNS.
- **Contraseña**: la contraseña de acceso a nuestra cuenta.
- **Host**: es el dominio que tenemos ya registrado.



Por ejemplo, en el caso de No-IP no tendremos que introducir la URL del proveedor, solamente con el usuario, contraseña y el host DDNS es suficiente para actualizarlo.

Cómo configurar el modo puente o bridge

En este router configurar el modo puente o bridge es realmente complicado, y es que el operador DIGI ha puesto serias dificultades para poder hacerlo. Por ejemplo, el operador Movistar o O2 lo facilitan a través de su menú de configuración básico, para que cualquier cliente pueda ponerlo en modo monopuesto y poner su propio router. DIGI también facilita las cosas bastante en las modalidades de 500Mbps o 1Gbps de velocidad, teniendo una ONT y router por separado, sin embargo, en esta PRO-DIGI de 10G lo tenemos muy difícil, pero no imposible, gracias a un maravilloso **script de Alez** donde nos facilita enormemente esta tarea.

Lo primero que debemos hacer es **instalar una máquina virtual con VMware Workstation o VirtualBox con Linux**, en nuestro caso, hemos usado la última versión de Debian para hacer este tutorial y también para hacerlo en nuestro propio router. En Internet hay multitud de información sobre cómo configurar una máquina virtual. Es muy importante que el adaptador de red esté configurado en «bridge» para que la máquina virtual obtenga directamente una dirección IP del router, y que no estemos en un entorno NAT virtualizado. El resto de opciones las puedes dejar como en los diferentes titulares.

Una vez que hayas instalado Linux, tendrás que seguir los siguientes pasos que os vamos a indicar.

Lo primero que debes hacer es asegurate de que tienes todo el software actualizado, puedes ejecutar la siguiente orden:

```
sudo apt update
```

Si hay algún paquete con actualizaciones, entonces tienes que ejecutar:

```
sudo apt upgrade
```

Una vez hecho esto, tendrás que bajarte el repositorio localmente para ejecutar el script principal, para ello debes hacer lo siguiente:

```
git clone https://github.com/alez-repos/ztef8648p.git
```

También debes asegurarte de que tienes todo el software necesario instalado en tu Linux, puedes ejecutar la siguiente orden:

```
sudo apt install cifs-utils python3 pip python3-pip
```

Una vez hecho esto, y para evitar que nos devuelva errores cuando ejecutemos el pip de instalación del software de Python3 que necesitamos, vamos a ejecutar la siguiente orden:

```
mv /usr/lib/python3.11/EXTERNALLY-MANAGED /usr/lib/python3.11/EXTERNALLY-MANAGED.COPIA
```

Ahora debemos meternos en la carpeta correspondiente para instalar el software adicional:

```
cd ztef8648p/supertools
```

Instalamos el software adicional que necesitamos para que funcione correctamente.

```
python3 -m pip install -r requirements.txt
```

Ahora ejecutamos la orden siguiente para ejecutar el script

```
python3 zte-supertool.py --nousb
```

En el script nos preguntará si queremos ejecutar una shell en el router y ejecutar comandos, o bien descargar la configuración y descifrarla, para tener todos los datos en nuestro poder. Nosotros hemos elegido la opción «1», y nos pedirá la contraseña del usuario «user», por defecto es «user» la clave, así que si no la has cambiado será esta la contraseña.

En la siguiente imagen puedes ver cómo debería salir:

```
root@debian:/home/bron/ztef8648p/supertool# python3 zte-supertool.py --nousb
ZTE F8648P supertool by alezz!
[nousb]: Running in nousb mode
[detect_router]: Checking if gateway (192.168.1.1) is a ZTE F8648P router
[detect_router]: It looks like 192.168.1.1 is a ZTE F8648P router
What do you want to do? [1=root shell,2=config decript]
1
What is the user password? [default: user]
user
[Login]: {"sess_token":"wpgb9dD3gj1EOwnF6cgRf9a0","login_need_refresh":true}
[Samba_post]: Setting samba status 0 (0=off, 1=on)
[Samba_post]: Setting samba status 1 (0=off, 1=on)
[nousb]: Waiting 2 seconds for server startup...
[nousb]: Created dest/ mountpoint
[nousb]: Mounted router smb on dest/
[nousb]: Symlink copied
[nousb]: Nc copied
[nousb]: Unmounted router smb
[nousb]: Deleted dest/ mountpoint
[Samba_post]: Setting samba status 0 (0=off, 1=on)
[Samba_post]: Setting samba status 1 (0=off, 1=on)
[Getlanip]: Acquired local IP 192.168.1.133
[Prepare_payload]: payload.sh ready
[Prepare_testsmb]: test.smb.conf ready
[Samba_pwn]: Waiting 2 seconds for server startup...
[+] Trying to bind to :: on port 3339: Done
[+] Waiting for connections on :::3339: Got connection from ::ffff:192.168.1.1 on port 42329
[Samba_pwn]: Connecting
[Samba_pwn]: Uploading payload.sh
[Samba_pwn]: Uploading test.smb.conf
[Samba_pwn]: Waiting for port 3339/tcp to be opened
[Samba_pwn]: Opening shell
[*] Switching to interactive mode
```

Ahora ya podemos ejecutar diferentes comandos como administrador, lo primero que debemos hacer es poner la clave de administrador como «admin» para entrar con todas las opciones:

```
sendcmd 1 DB p DevAuthInfo
sendcmd 1 DB set DevAuthInfo 0 Pass admin
sendcmd 1 DB save
```

Después, es muy recomendable cambiar la región del router para tener acceso al modo bridge vía web directamente:

```
echo "current : 173" > /userconfig/flag_type
```

Una vez hecho esto, lo que debemos hacer es quitar el cable de fibra del router, y ejecutar la siguiente orden para sacar los datos de usuario y clave PPPoE:

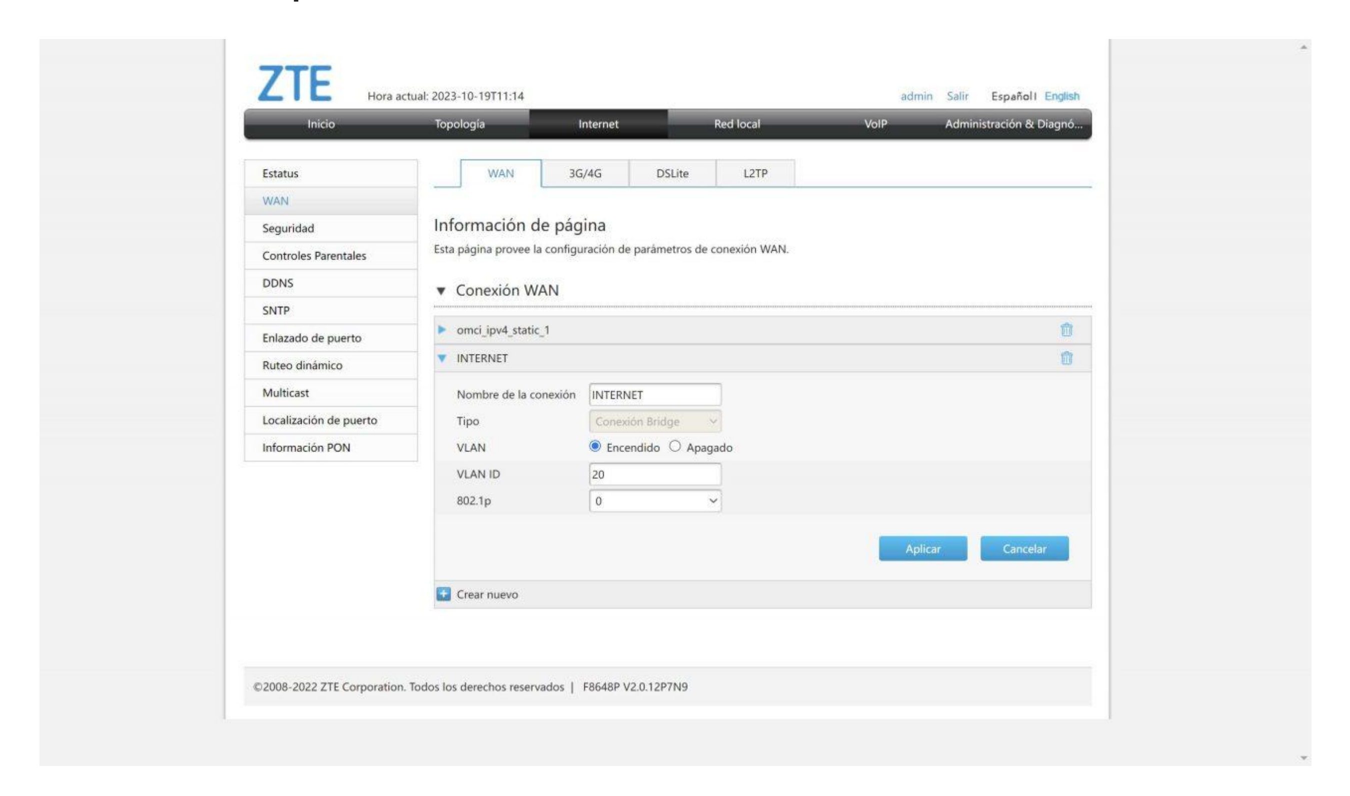
```
tcpdump -i any -A pppoes
```

Una vez que esto esté en ejecución, ponemos el cable de fibra y esperamos 1 minuto hasta que se establezca la conexión PPPoE. En la pantalla nos aparecerá tanto el nombre de usuario como la contraseña en texto plano, el nombre de usuario tiene el siguiente aspecto «**9_DIGITOS@digi**» y la contraseña está justo al lado y está formado por números y letras, pero no símbolos.

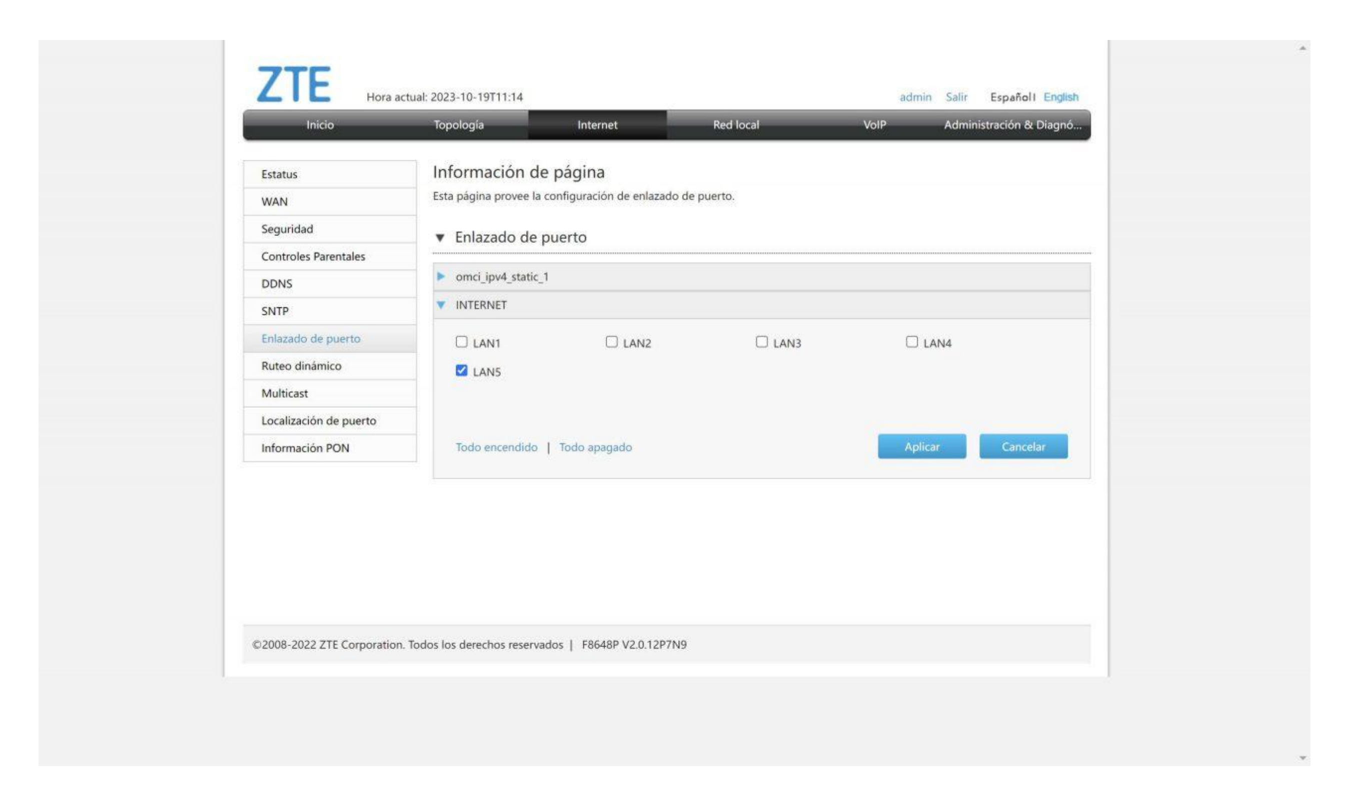
Cuando ya tengamos la contraseña del PPPoE, podemos poner el router en modo bridge. Los pasos para hacer esto consisten en irte a la sección de «Internet / WAN», aquí tienes que eliminar la conexión llamada «INTERNET» y crear una nueva desde cero. La configuración que debes realizar en esta nueva conexión consiste en:

- **Nombre de la conexión**: INTERNET
- **Tipo**: Conexión Bridge
- **VLAN**: encendido, y ponemos un «20» que es el VLAN ID.

Pinchamos en «**Aplicar**«:



Ahora nos vamos a la sección de «**Internet / Enlazado de puerto**«, y en la sección de «**INTERNET**» debemos seleccionar únicamente la interfaz física donde queremos que esté el bridge, al ser un router 10G y con una conexión de fibra, tenemos que usar el puerto 10GBASE-T para no tener ningún tipo de cuello de botella. Entonces lo que hay que hacer es seleccionar únicamente el puerto LAN5 y pinchamos en aplicar.



Si queremos acceder a la web de administración del router nuevamente, no podremos hacerlo a través del **puerto LAN5** porque está en bridge, pero sí podemos hacerlo a través del resto de puertos físicos sin ningún problema. Por último, lo que también deberías hacer es quitar el Wi-Fi del router para que no ocasione interferencias con el router WiFi principal que vayas a poner. Debes tener muy en cuenta que, seguramente, el nuevo router que vayas a poner no te proporcione los 8Gbps de velocidad, e incluso ni siquiera llegue a 3Gbps debido al uso del PPPoE, por lo que tenlo muy en cuenta.

Hasta aquí hemos llegado con esta guía completa de las principales opciones de configuración que debes hacer en el router ZTE ZXHN F8648P de DIGI 10G.

¿Cómo puedo sustituir este router por otro?

DIGI no permite sustituir este router con ONT integrada de manera sencilla, como hemos visto anteriormente, será necesario «hackearlo» para sacar los **datos de PPPoE y VoIP** si es que tienes contratada la telefonía. Estos datos son totalmente necesarios si quieres sustituir por completo el router de DIGI por uno propio, como un AVM FRITZ!Box 5590 Fiber o 5530 Fiber que son completamente compatibles con la fibra de XGS-PON del operador. Para poder sustituir el router del operador, necesitarás recopilar la siguiente información:

- **SN utilizado por DIGI en nuestra conexión**. Es el número de serie del router ZTE que nos han instalado en casa, podemos verlo directamente en la pegatina, o bien a través de la web «Mi DIGI», donde nos mostrará el router que nos han instalado. Este SN deberás incorporarlo en la configuración del nuevo router que instales, porque si tiene un SN diferente no va a funcionar, es algo totalmente necesario.

- **PPPoE**: el operador usa el tipo de conexión PPPoE, así que necesitarás tener tanto el nombre de usuario como la contraseña. Esta información solamente la podrás sacar del router ZTE ya que no te proporcionarán las credenciales. El operador DIGI en las conexiones de 500Mbps o 1Gbps sí proporciona los datos PPPoE, pero en la conexión de 10Gb no es así. Si por casualidad tienes 1Gbps y quieres pasarte a 10Gb, puedes pedir los datos de PPPoE previamente ya que serán exactamente los mismos, no cambiarán. Para poder extraer estos datos del router necesitarás «hackearlo», hacer un tcpdump de la conexión PPPoE antes de conectar la fibra, y ver la línea de código relacionada con la autenticación.
- **VoIP**: en muchos casos los usuarios deciden no contratar el teléfono fijo, en nuestro caso personal, tampoco lo hemos contratado. No obstante, si te interesa tener el fijo, también tendrás que extraer los datos de la VoIP a través del router ZTE.

Nosotros hemos conseguido sustituir el router ZTE por un AVM FRITZ!Box 5590 Fiber, y el funcionamiento es perfecto, aunque lógicamente nos vemos limitados a 2.4Gbps de velocidad ya que solamente dispone de un puerto 2.5G para la LAN, no tenemos un puerto 10Gb como sí ocurre con este router que proporciona el operador. Muy pronto AVM lanzará un router con un puerto 10Gb para no tener estos problemas de cuello de botella en la red cableada, pero hasta entonces, existen pocas alternativas en el mercado. Nuestra recomendación es que pongas el modo bridge y posteriormente conectes un router potente que tenga aceleración de PPPoE para no tener problemas.